2019 22nd International Conference on Computer and Information Technology (ICCIT), 18-20 December, 2019

Malicious Nodes Detection based on Artificial Neural Network in IoT Environments

Mirza Akhi Khatun
Computer Science & Engineering
Jagannath University
Dhaka, Bangladesh
mirza_akhi@hotmail.com

Niaz Chowdhury
Knowledge Media Institute
The Open University
Milton Keynes, United Kingdom
niaz.chowdhury@open.ac.uk

Mohammed Nasir Uddin
Computer Science & Engineering
Jagannath University
Dhaka, Bangladesh
uddinmn@mail.ru

***Abstract*—The central promise of the Internet of Things (IoT) is to accelerate the interaction with surroundings. Appliances such as smartwatches, smart bulbs, thermostats, fitness trackers, next-generation vehicles, and so on have gained the ability to communicate and accept instructions from outside with the help of various embedded devices. While doing so, they almost always operate with little to no human interaction. These embedded devices, alongside a lot of benefits, also bring forth several security challenges. From the manufacturers' point of view, performance and production remain the top priority leaving security a less addressed problem. This practice has manifested itself in the form of various attacks including the Distributed Denial of Service (DDoS) where malware prepared with the aid of malicious nodes in IoT devices are used to carry out the attack. It is, therefore, essential to comprehend the nature of these attacks and swiftly identify infected devices to combat this situation. Machine Learning, or more particularly a branch of this technique commonly known as Deep Learning, has already demonstrated its outstanding potentials while administering with the heterogeneous data of diverse sizes. Using the Artificial Neural Network (ANN), this work suggests a method of detecting malicious nodes in IoT environments. The contribution of the paper is in two-fold. First, it classifies the usual and malicious patterns of IoT devices in the network, and second, describes a scheme for successfully detecting malicious nodes with 77.51% accuracy.**

***Index Terms*—Internet of Things (IoT), Machine Learning, Artificial Neural Network, Device Type Identification**

I. Introduction

The Internet of Things (IoT) provides immense opportunity for accomplishing a large amount of data from smart objects used in our day to day activities. These objects could have been smartwatches, smart bulbs, thermostats, solar panel, fitness trackers, smart glasses, and so on [1], [2]. Connected devices equipped with sensors or actuators identify their surroundings, perceive what is going on, and perform correspondingly [3], [4].

There is an upswing growth of IoT devices around the world where businesses require running, testing, debugging and securing these connected devices in real-time. This job, however, is challenging because of three reasons: first, there exists a lack of control over the devices due to being remotely deployed, and second, the heterogeneous nature of the environment contributes to this problem by making the communication more difficult. There also exists a third and perhaps a bigger challenge in the form of securing devices and the network from bugs, vulnerabilities, and malicious threats. This latter challenge needs identifying the abnormal behaviour of IoT devices to develop adaptive and innovative anomaly detection techniques and malicious nodes detections.

Device fingerprinting approaches such as offline log analysis, statistical anomaly discovery and rule-based detection have been amongst the widely used techniques to deal with these challenges. They extract behavioural features to make decisions where security and privacy remain to be informative of aspect structures raise on machine learning through the prism of the classical confidentiality, integrity, and availability (CIA) model [5].

The techniques mentioned above, however, fail to provide a real-time device classification solution that Artificial Neural Network (ANN)-based feature extraction driven approaches do. The process though is not as straightforward as it sounds. To the best of our knowledge, there exists no effective method in the literature that stress on studying long-term behaviour of devices; hence requires extracting statistical features occupying the behavioural snap of raw IoT traffic data [6]. Furthermore, there have been no significant work in the past on the area of extracting features from the packet headers of IoT traffic data to classify malicious nodes making our research one of the first attempts.

Our solution originates on the foundation that features extracted from the packet headers of random nodes can be combined with the features of the devices that had undergone long-term behavioural analysis. This approach leads us to build a technique capable of identifying malicious devices as opposed to nodes behaving usually in the IoT networks. The paper analyzes data, including the frames, from the IoT devices to develop malicious nodes detection method based on the ANN followed by building a threat model to understand the potential attacks. This method can be leveraged further in several security aspects such as device isolation, in-depth log analysis, packet header inspection, and so on.

A. Problem Statement

Experts assume that unknown attacks and vulnerabilities will increase with the growing usage of wireless connectivity

978-1-7281-5842-6/19/$31.00 ©2019 IEEE

in the near future [7]. As such, Wi-Fi networks, particularly public networks, and smart appliances attached to them at airports, hotels, restaurants, and so on are likely to experience security concerns. That said, it does not nullify the possibility of having attacks launched at the private networks and home appliances. Any interface having a weak password or allowing users to connect on the fly without the need for one potentially allows the attacker to impersonate as a device and attempt to harm the system.

Attacks on smart devices are not complicated. The attackers could potentially utilize household appliances with network connectivity to launch IoT-based cyber-attacks. Gadgets such as home routers, refrigerators, televisions, PlayStations and so on had been used as a stage to send thousands of phishing and spam emails in recent time [8], [9]. Let suppose several bulbs are connected in a network. An attacker impersonating as a bulb could enter the system and begin to exchange data just like a regular bulb. There exists no easy solution to detect such anomaly, particularly if the number of devices is enormous. This problem motivates us to suggest a basic plan that will be competent in identifying security threats within smart appliances surroundings at network-level.

B. Contributions

In this paper, we proposed a method for detecting malicious nodes of IoT devices. In doing so, we generated the dataset to implement our process and analyzed performance evaluation using an ANN *classifier*, based on the features extraction of the traffic data of individual smart bulbs. The contributions of the work are as follow:

- For classification, our method depends only on Wi-Fi network traffic data. To the best of our knowledge, this is the first attempt to use network traffic data of smart bulbs for an ANN-classifier to detect malicious nodes in IoT environments.
- We implemented the focused system and indicated the performance of our classifiers using only smart bulb IoT devices. Further, these devices' descriptions can be found in Table II. It is representative of real-world usage.
- Traffic data was captured over several months in different networks. The device was operated by a smartphone app and located in the commonplace, e.g., a bulb in the office lab, reading room, and drawing room. First of all, we collected data from the bulb; then, we have tried to comprehend the data frame of the device.
- Our method is proposed by using this kind of smart bulb, which shows how the attacker will try to attack the system (e.g., computer, router, server, database, etc.). Therefore, based on this concept, we develop a threat model, and have provided an explication of the model.

The rest of this paper is organized as follows: In section II, we describe a threat model along with the possible types of attack. Section III discusses the existing research on device classification in IoT environments. We then explained the proposed methodology process to detect the malicious nodes based on Artificial Neural Network (ANN) in section IV. In section V, we evaluated the proposed solutions and compared our results to existing works, and the paper concludes in section VI.

II. Threat Model

The threat model is a useful technique to avoid the vulnerabilities and comprehend the system in IoT environments. It helps to decide on IoT application because of IoT environments being immensely complicated [10].

While developing the threat model, we focused on public Wi-Fi networks. Such networks were initially intended to be a local-area network with a mesh topology having each device connected to an access point [11]. For example, in restaurants, customers' smartphone data is crucial, and similarly, restaurants' information which kept on their system is sensitive and confidential. In such cases, IoT devices can be mishandled to for illicit purposes. If smart bulbs intrinsically share data, an attacker can compromise and use these bulbs for various attacks. In this study, we consider the IoT security attacks as shown in Table I.

Serial No.	Types of Attack	Name of Attacks
1	Spoofing	IP Spoofing MAC Spoofing
2	Sniffing	Packet Sniffing
3	Malware	Backdoor, Information Steal, User ID Password Steal, Spam, Worm
4	Impersonation	Impersonation
5	DoS	Ping of Death Land Attack

TABLE I: Threat Model

- **Spoofing:** A spoofing node impersonates a legal IoT device with its information i.e., Media Access Control (MAC) address and IP address spoofing to obtain unauthorised access to the IoT system [12].
- **Sniffing:** Sniffing is a common network security attack in that a device proceeds important data from the network [13]. This attack is regular in wireless networks and settlements behind-the-scenes of transmissions. When the attacker will be joining in the network by spoofing or impersonating as an IoT device, attacker will try to sniff to obtain the important information such as password (Computer, e-mail, FTP, database).
- **Packet Sniffing:** Packet sniffing means the attacker tries to observing each packet that traverses the network. If the packets are not encrypted with strong network security then the attacker might loot the data and analyze it. Because this type of IoT devices do not use any encryption method in the network, they can be very weak to sniffing attacks.
- **Malware:** A malware attack is a bit of malicious program which can be used for criminal purposes by an attacker. It begins with sending GET requests to the server to fetch port-mapping parameters according to punch holes through NAT and reveal the accumulated local devices [14]. Lately, a vast number of malwares have been

developed to attack IoT devices. This type of attack is the combinations of multiples malicious program such as backdoor, information steal, spam, and worm. backdoor attack could be sent harmful data anytime in the system (computer, router, database, server, smart phone) while worms and viruses are some of the dangerous malwares used by adversaries to exploit the users [15].

- **Impersonation Attack:** The attackers want to impersonate themselves either as a physical node or a unit of implicit node [16]. Such attacks are particularly easy to launch in IoT environments and can root significant harm to system performance [17]. Suppose, S is the source and D is the destination and R is the intermediate IoT node is represented in Fig. 1. A malicious node exchanged its identity with intermediate IoT node (R) and veils its actual identity with other IoT nodes. Sometimes impersonation attacks are the initial steps for launching a full throttle attack.
- **DoS Attack:** The purpose of a DoS attack is to make a service unavailable such that client can not access the system/network [18]. A Denial of Service (DoS) attack that blocks up large memories on the target system aims it to crash or reboot. An Attacker can attack the system by impersonating as a bulb and then will try to send malicious information to the router. Suppose, the attacker sends the data packet of a bulb, and Firewall relieves it by assuming as bulb's data packet. However, the packet's payload may contain information enough to attack the router.
- **Ping of Death:** The attacker tries to send an over-sized ping packet to the destination to bring down the target system because of the lacking of systems ability to handle large ping packets [19].

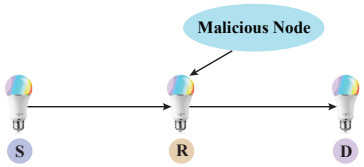

Fig. 1: Impersonation Attack

- **Land Attack:** A Land attack is also a type of DoS attack that contains sending an unusual malicious spoofed data packet to a system or a network, attempts it for jamming [20].

III. Related Work

This section presents the previous work of devices classification based on various algorithms. Machine learning is a research area that generally focuses on the performance, learning methods and algorithms. IoT devices classification has been used enormously based on Machine Learning techniques. For example, previous work has focused on device classification for IoT network traffic data [21].

Nathalie *et al.* Proposed an ML model to detect and filter poisonous data for the smart factory network. This paper presents provenance-based defense for cases into two categories datasets partially trusted and entirely untrusted dataset. The authors used the SVM algorithm for detecting poisoning attacks. SVM algorithms are not faster in classification [22].

Farook Shaikh *et al.* described an ML model for classification the IoT devices. The authors have collected darknet data from the Center for Applied Internet Data Analysis [CAIDA] dataset, but this model trained only on malicious data, which mainly focused on malicious activity. So, this solution does not represent explicitly of IoT benign data because of cannot use any realistic setup for IoT devices to collect benign data [23].

Meanwhile, the authors used several supervised learning algorithms to detect anomalies in IoT environments. Timčenko *et al.* has collected IoT data from UNSW-NB15 dataset, but did not represent any practical setup to collect IoT data. Several supervised algorithms to take more time to train for large dataset [24].

In a later work proposed a method for classifying IoT devices connected to the network, based on Random Forests for features selection. This algorithm consist combines of the Decision Tree. Yair Meidan *et al.* has collected traffic data from IoT devices, only two methods were appointed in lab A and lab B. There are most important features, i.e., TCP packet time to live (minimum), TCP packet time to live As a result (first quartile), and TCP packet time to (live average). The method has trained from lab A and tested from another lab B. There were no unusual IoT devices and does not represent explicitly on malicious data [25].

IV. Proposed Method

We proposed the method to detect malicious nodes of an IoT device such as smart bulbs based on Artificial Neural Network (ANN). We applied and compared the performances of several supervised algorithms, including ANN classifiers. We have measured the performances of the selected algorithms with our dataset. Our method consists of the following pseudocode in Algorithm 1.

A. Data Acquisition

Data acquisition performs the role of data collection from IoT devices to make dataset. We captured the raw traffic data in *pcapng* format from smart bulbs (see Table II). To ensure that we have generated the training dataset with attack data and benign data as [.csv] file format and trained an ANN using this dataset. Whereas there was no unusual device. For this reason, we have just modified the original data and then converted it into attack data. For example, In a data packet the previous captured frame was 0.186248. After that, it was changed about last three or four-digits for attack data. For another example, the original payload length was 183 then we have put 184 or sometimes 182 for attack data. To build a dataset, we must have a clear pattern of everything that we can use [26]. On the other hand, we can tell that hackers

Algorithm 1: Pseudocode for Backpropagations

Data: *Dataset*, a dataset consisting of the training attributes for classification, L, a parameter called 'learning rate' and *classifier*, a multi-layer Artificial Neural Network (ANN)
Result: A trained Artificial Neural Network (ANN)
while *final condition is not fullfilled* **do**
  for *each training tuple* X_{train} *in Dataset* **do**
    for *each Input layer* m **do**
      $O_m = I_m$
    end
    for *each hidden/output layer* m **do**
      Preparing Inputs:
      $I_m = \sum_n (w_{nm} \cdot O_n) + \theta_m$
      Computing outputs for each m:
      $O_m = Sigmoid\ activation$
    end
    for *each unit* m *in the output layer* **do**
      Back propagation of error:
      $E_m = O_m(1 - O_m)(T_m - O_m)$
    end
    for *each* m *from the last to the first hidden layers* **do**
      $E_m = O_m(1 - O_m) \cdot \sum_h (E_h w_{mh})$
    end
    for *each weight in classifier* **do**
      $w_{nm} = w_{nm} + (L) \cdot E_m \cdot O_n$
    end
    for *each bias* θ_m *in classifier* **do**
      $\theta_m = \theta_m + (L) \cdot E_m$
    end
  end
end
Prediction:
if $y_{pred} > 0.5$ **then**
  $result \rightarrow$ *hacked*
else
  $result \rightarrow$ *not hacked*
end

cannot send the data packets simultaneously as like a normal device. Definitely, there will be the timing difference between the usual device and the unusual device.

B. Data Preprocessing

The main reason for the Data Preprocessing (DP) is to experiment the data stability in ANN classifier. Data preprocessing is a data mining method which involves converting raw data into an understandable format. It is a very crucial step in the machine learning process. Generally, real-world data is imperfect, inconsistent or missing in certain behaviours or trends, which is likely to confirm various errors. Data preprocessing also is a demonstrated technique for resolving these types of issues. Data preprocessing makes raw data for further processing.

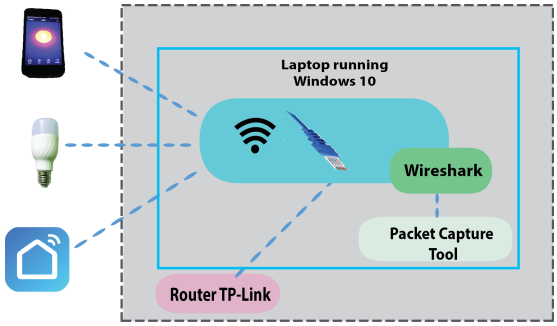

Fig. 2: Data Capturing Configuration

C. Feature Extraction

One of the most important steps is to select the most relevant features in any ML design process [27]. Whenever a data packet arrives, we create a baseline profile from the raw data packets of devices before the feature extraction. In baseline profile, we extract the set of 21 features. Malicious nodes detection technique is based on this feature extraction process. So, we have found the most essential six features from our baseline profile. The raw data packets are not enough to take the input to learning algorithm because of the this data containing information such as source/destination IP address, source/destination port, protocol which bases noise and over-fitting in the learning algorithm.

For this reason, we created a feature extraction method which is valuable to learning algorithm of IoT devices. Our selected feature consists of the following:

- **Period Time:** The time respective to period time or epoch. It is important for a packet which contains the interval of time.
- **Previous Captured frame:** The time respective to the previous captured frame.
- **Previous Displayed Frame:** The time respective to the previous displayed frame.
- **Time Since Reference:** The time since reference is the beginning point for all next packet time computation.
- **UDP Payload Length:** This is the length of the payload conveyed inside a UDP data. In other words, this is the main length of the data sent by a specific device.
- **Total Length:** This device provides the total length at 182 and sometimes 183.

D. Train an Artificial Neural Network

As our base malicious nodes detection, we used an Artificial Neural Network Classifier for each smart bulb. This classifier is a biologically motivated computational technique which consists of a vast number of neurons. The neurons are interconnected and operate in parallel. Neural Network consists of a set of process components that are incredibly interconnected and modify a collection of inputs to a group of desired outputs [28]. All neurons are related to other neurons through strong communication links, which represent the neuronal structure, all with a combined weight. The weights constitute

in evolution being used by the network to solve a problem, but in a typical way, layers are neuron category. The neural network architecture which was selected for a self-organizing feature map that use one layer of neurons to represent data from a selected domain inside the type of a geometrically organized feature map [29].

The training stage is the initial step for devices classification. The Artificial Neural Network classifier is initially trained with the labeled dataset such as the supervised approach for the device classification. The training dataset restrains all the features needed to classify malicious nodes.

During the training procedure, as the backpropagation networks frequently try to improve internal relationships among the neurons to arrange the training data systematically. The hidden layers of backpropagation are connected to a particular characteristic of the nearer pattern as an outcome of the training. We note that the network can have more than a single hidden layer.

E. Malicious Nodes Detection

In this part, The neural network performs dot product for test dataset with a weight set, with the dot product summation method add bias. Activation function is applied to the hidden layers and the output layers. We used sigmoid activation function *(1/(1 + exp (-x)))* to the various interrelation weights. The activation function provides the output whether malicious nodes are detected or not. We used fourth hidden layers to test how accurately neural network was trained. Our recommendation method – *Malicious Nodes Detection* with an organizational codebase which is based on *Python*. To further demonstrate and generalize our findings, we have created a repository on GitHub [30].

V. Performance Evaluation

This section illustrates the outcome of this work as well as a comparative analysis with existing methods to demonstrate the uniqueness and supremacy of the proposed method.

Device Label: Device	Model	Category	Connectivity
Fcmila Bulb	E-B06-A8-202	Smart Bulb	Wifi
Fcmila Bulb	E-Y24-B5-301	Smart Bulb	Wifi

TABLE II: Device Description

A. Experimental Setup

We analyzed our approach on the newest IoT devices, listed in Table II, available in the market. The device label consistent with the unique accessory given to this device type. The category is compatible with the general classification for both devices.

To enable traffic data capture from the smart bulb, we established a bridge over the software setup as shown in Fig. 2, operating a general-purpose laptop running Windows 10 on an Intel processor with 8 GB RAM. This configuration allowed us to capture all traffic data, including the traffic passing along the network router. Over a couple of several months, we collected traffic data from bulbs in several networks. We used the *Wireshark* tool to collect data and packets were in *pcappng* format. In our pseudocode, the training dataset represents *Dataset* and for each training tuple defines as X_{train} in *Dataset*. Each of the traffic data is a set of UDP packets with source IP address due to DHCP and destination IP address was always same.

B. Metrics for Performance Evaluation

This section demonstrates the accuracy measure of the proposed classification system and comparative analysis of the performance relative to existing works using ANN classifier. The accuracy is calculated in the equation.

$$\text{Accuracy} = \frac{Number\ of\ correctly\ classified\ nodes}{Number\ of\ nodes\ in\ test\ dataset} * 100\% \tag{1}$$

Thus, the error rate is calculated in equation

$$\text{Error Rate} = \big(100\ -\ Accuracy\big) * 100\% \tag{2}$$

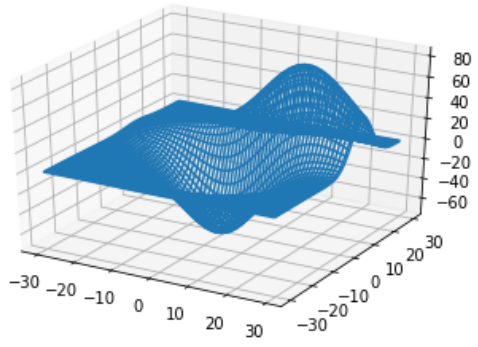

Fig. 3: Detected and Undetected Nodes

C. Artificial Neural Network (ANN) Classifier

The feed forward neural network with backpropagation training algorithm is deployed as the classifier. Though the number of hidden layers is four, but all the hidden neurons use the sigmoid function. The reason for using the sigmoid function that grips the output into the range from 0 to 1 and the function is differentiable; hence, the method is performed to predict the probability as an output. This method can find the slope of the sigmoid curve at any two points presenting the detection of the malicious nodes.

The proposed methodology can detect 77.51% accurate malicious nodes with an error rate of 24.49%. The performance matrices of the final classification results based on Artificial Neural Network (ANN) are shown in Fig. 3. If we increase the size of the training data, more accuracy can be obtained. The existence of a large volume of data is always useful for machine learning models. For example, Hasan et. al. collected a dataset of 357,952 samples from kaggle helping them to obtain much higher accuracy with ANN classifier [31].

D. Comparative Assessment

The results comparing the proposed method with four others are shown in Fig. 4. It demonstrates that the accuracy and error rate of ANN (that scored 77.51% and 24.49%) is better or at least competitive than the earlier results.

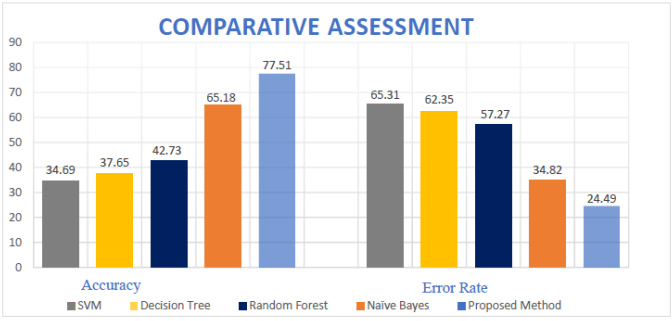

Fig. 4: Comparative Assessment

The comparison demonstrates that our proposed method is best suited in all purposes.

VI. Conclusion

To summarize, this paper has demonstrated how Artificial Neural Network (ANN) can be performed to analyze the network traffic in sequences for detecting malicious nodes in IoT environments. We also demonstrated the reliability of our approach by classification accuracy. The accuracy has been gained when training and testing were performed on the dataset. The ANN classifiers achieved 77.51% in the detection of malicious IoT nodes. Besides, we analyzed and developed a threat model to detect the attempted adversarial attacks, although hypotheses rather than practical.

One of the limitations is the variety of smart bulbs or IoT devices which communicates via Wi-Fi. Therefore, other IoT devices related to technology like Zigbee or Zwabe were not available. In the future, we plan to diversify the devices used in our research.

References

[1] B. Schneier, "The internet of things will upend our industry." *IEEE Security & Privacy*, vol. 15, no. 2, p. 108, 2017.

[2] N. Chowdhury, B. Price, A. Smith, G. Kortuem, J. v. d. Linden, and J. Moore, "Ev charging: separation of green and brown energy using iot," in *ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*. ACM, 2016, pp. 674–677.

[3] Q. Zhou and J. Zhang, "Research prospect of internet of things geography," in *2011 19th International Conference on Geoinformatics*. IEEE, 2011, pp. 1–5.

[4] N. Chowdhury, B. A. Price, A. Smith, D. Gooch, and J. v. d. Linden, "50 shades of green and brown: Comparing grid carbon intensity with consumption for households with pv generation and battery storage," in *IEEE 6th Conference on Technologies for Sustainability Technologies*. IEEE, 2018.

[5] N. Papernot, P. McDaniel, A. Sinha, and M. P. Wellman, "Sok: Security and privacy in machine learning," in *2018 IEEE European Symposium on Security and Privacy (EuroS P)*, April 2018, pp. 399–414.

[6] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.

[7] M. E. Aminanto and K. Kim, "Detecting impersonation attack in wifi networks using deep learning approach," in *International Workshop on Information Security Applications*. Springer, 2016, pp. 136–147.

[8] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *IEEE World Congress on Services*. IEEE, 2015, pp. 21–28.

[9] I. Proofpoint, "Proofpoint uncovers internet of things (iot) cyberattack," 2014.

[10] N. Chowdhury and L. Mackenzie, "Development of a threat model for vehicular ad-hoc network based accident warning systems," in *ACM 7th International Conference on Security of Information and Networks*. ACM, 2014, pp. 447–452.

[11] M. Afanasyev, T. Chen, G. M. Voelker, and A. C. Snoeren, "Analysis of a mixed-use urban wifi network: when metropolitan becomes neapolitan," in *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*. ACM, 2008, pp. 85–98.

[12] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "Iot security techniques based on machine learning," *arXiv preprint arXiv:1801.06275*, 2018.

[13] A. Kulshrestha and S. K. Dubey, "A literature reviewon sniffing attacks in computernetwork," *International Journal of Advanced Engineering Research and Science (IJAERS)*, vol. 1, no. 2, 2014.

[14] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2016, pp. 195–200.

[15] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the ip-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[16] O. El Mouaatamid, M. Lahmer, and M. Belkasmi, "Internet of things security: Layered classification of attacks and possible countermeasures," *electronic journal of information technology*, no. 9, 2016.

[17] R. Regan, J. Manickam, and M. Leo, "A survey on impersonation attack in wireless networks," *INTERNATIONAL JOURNAL OF SECURITY AND ITS APPLICATIONS*, vol. 11, no. 5, pp. 39–48, 2017.

[18] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[19] E. Gelenbe and Y. Yin, "Deep learning with dense random neural networks," in *International Conference on Man–Machine Interactions*. Springer, 2017, pp. 3–18.

[20] A. Fadia, *Network Security*. Macmillan, 2006.

[21] Y. Meidan, M. Bohadana, A. Shabtai, J. D. Guarnizo, M. Ochoa, N. O. Tippenhauer, and Y. Elovici, "Profiliot: a machine learning approach for iot device identification based on network traffic analysis," in *Proceedings of the symposium on applied computing*. ACM, 2017, pp. 506–509.

[22] N. Baracaldo, B. Chen, H. Ludwig, A. Safavi, and R. Zhang, "Detecting poisoning attacks on machine learning in iot environments," in *IEEE International Congress on Internet of Things (ICIOT)*. IEEE, 2018, pp. 57–64.

[23] F. Shaikh, E. Bou-Harb, J. Crichigno, and N. Ghani, "A machine learning model for classifying unsolicited iot devices by observing network telescopes," in *14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 938–943.

[24] V. Timčenko and S. Gajin, "Machine learning based network anomaly detection for iot environments."

[25] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. D. Guarnizo, and Y. Elovici, "Detection of unauthorized iot devices using machine learning techniques," *arXiv preprint arXiv:1709.04647*, 2017.

[26] A. Gonfalonieri, "How to build a data set for your machine learning project," Tech. Rep., 2019.

[27] A. L. Blum and P. Langley, "Selection of relevant features and examples in machine learning," *Artificial intelligence*, vol. 97, no. 1-2, pp. 245–271, 1997.

[28] J. Cannady, "Artificial neural networks for misuse detection," in *National information systems security conference*, vol. 26. Baltimore, 1998.

[29] K. Fox, "A neural network approach wowards intrusion detection," *Tech. Rep.*, 1990.

[30] "Malicious Nodes Detection with ANN," Tech. Rep., 2019, accessed: August 9, 2019. [Online]. Available: https://github.com/mrizaakhi/MaliciousNodesDetectionwithANN.git

[31] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in iot sensors in iot sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, 2019.